EXHIBIT 8

Trials@uspto.gov
571-272-7822

Paper No. 8

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS INC.,
Petitioner,

v.

TEXTILE COMPUTER SYSTEMS, INC.,
Patent Owner.

Case IPR2017-00296
Patent 8,505,079 B2

PATENT OWNER'S PRELIMINARY RESPONSE UNDER 37 C.F.R. § 42.107

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Cases **Pages(s)**

Statutes

Regulations

LIST OF EXHIBITS

TEXTILE'S EXHIBIT NUMBER	DESCRIPTION
2002	Declaration of Gopal Nandakumar
2003	Declaration of Richard Oglesby

Patent Owner Textile Computer Systems, Inc., ("Patent Owner" or "Textile") hereby submits this Preliminary Response under 37 C.F.R. § 42.107 to Unified Patents Inc.'s ("Petitioner" or "Unified") Petition for *Inter Partes* Review of U.S. Patent No. 8,505,079 ("the ''079 Patent"), filed October 23, 2011.

I. <u>INTRODUCTON AND SUMMARY OF ARGUMENT</u>

Inter partes review is not appropriate in this case and Unified's Petition should be denied under 35 U.S.C. § 314(a) because Petitioner cannot establish a reasonable likelihood of success on any claim challenged. "The Director may not authorize an *inter partes* review to be instituted unless the Director determines that the information presented in the petition filed under section 311 . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged." 35 U.S.C. §314(a).

As detailed below, Johnson does not disclose each and every one of these features as arranged and recited in claims of the '079 Patent, either alone or in combination with Stambaugh (Ground 1) or Sellars (Ground 2). The Petition's proposed obviousness rejections therefore fail to articulate a sound basis for a legal conclusion of obviousness and do not establish a *prima facie* case of obviousness. Accordingly, the proposed obviousness rejections fail to comply with Patent Office Rules and Supreme Court precedent and the Petition should be denied. *See* 37 C.F.R. § 42.104(b)(5); *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S.

398, 418 (2007) (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

The following limitations of independent claim 1 (and analogs in claim 11) of are not taught by any of the prior art combinations cited in the Petition:

(1) receiving from "a requester **purporting to be an authorized user of a secured resource a request for access by an unauthorized service client to said secured resource**,"

(2) "**determining a key string known to both said secured resource and the authorized user** said requestor purports to be, said key string being adapted to provide a basis for **authenticating the identity** of said requester,"

(3) "receiving an **authentication credential from said unauthorized service client associated with said request for access, said authentication credential** having been provided to said unauthorized service client by said requestor," and

(4) **"evaluating said authentication credential to authenticate the identity** of said requester;

Petitioner asserts the recited "key string" (and consequently the recited "authentication credential") is merely "an ordered sequence of any subset of symbols selected from a set of symbols wherein each symbol forming the set may be represented in both a format that may be perceived by an end user 34 and a format that may be recognized by software or hardware that may be used to provide a basis for authenticating the identity of the requester." Petition at pps. 16; 52.

This argument misconceives the claimed invention and reads out a critical limitation in the ‘079 specification that prohibits the claimed “key string” from being the common identifier of the secured resource (including the primary account number or PAN to be accessed in a payment transaction) or any other value that could provide knowledge to allow the unauthorized service client to make ordinary use of the resource outside the system or to again have access to the secured resource within the system without again obtaining authorization from the authorized user. Petitioner’s overbroad proposed construction of “key string” alone is fatal to Petitioner’s prima facie case because neither the primary reference, Johnson, nor the other prior art references relied upon by Petitioner, alone or in combination with Johnson, expressly or inherently meet such a limitation much less the other claim limitations identified above of the claimed arrangement.

Petitioner, as will be detailed below, also fundamentally misapprehends the asserted prior art’s teachings relative to the system disclosed and claimed in the ‘079 patent, additionally failing to make any prima facie case in either of the two asserted grounds.

The ‘079 system enables an efficient and effective “mobile wallet” architecture which can be used to make normal credit card transactions without having to provide the merchant with credit card details.[1] The technology is

[1] “Normal” credit card processing here means that the merchant processes the credit

marketed by Textile under a suite of products called MySingleLink that Textile started developing in 2011. EX2002, Declaration of Gopal Nandakumar ("Nandakumar Decl.") at ¶¶ 3-5.

In contrast, Johnson describes an on-line version of the old certified check system. Likewise, Stambaugh describes an SMS based version of the old pre-paid reloadable merchant specific gift card system. And Sellars is a content protection system using encryption and likewise does not disclose a system like the '079 patent that enables normal credit card processing. Neither Johnson nor Stambaugh nor Sellars (nor any other prior art described by Mr. Mott) addresses the problem addressed by the '079 patent, which enables a normal credit card transaction to be conducted without the credit card holder needing to provide the merchant with a credit card number and which further prevents fraudulent credit card transactions by authenticating the actual credit card holder approved of the transaction. None of these (or any other systems described in the background of Mr. Mott's declaration) disclose the claimed system. EX2003, Declaration of Richard Oglesby in Support of Patent Owner's Preliminary Response ("Oglesby Decl.") at ¶¶ 11-14.

This filing is timely under 35 U.S.C. §313 and 37 C.F.R § 42.107 as it is being filed within three months of the date noticed. Textile, by submitting this

card transactions in the normal manner (just without having the credit card account number) without requiring some intermediary payment authority to pre-collect the funds.

response, does not waive its rights to add or modify arguments should the Board decide to institute a trial on this matter. Textile does not waive or admit any matters, arguments, contentions or other material presented in the Petition regardless whether they are addressed or rebutted in this response.

II. RELATED MATTERS

The ‘079 patent is currently involved in the following court proceedings identified by Petitioner: *Textile Computer Systems, Inc. v. Sabine Federal Credit Union*, Case No. 2:16-cv-01047 (E.D. Tex.); and *Textile Computer Systems, Inc. v. East Texas Professional Credit Union*, Case No. 2:16-cv-00702 (E.D. Tex.).

The ‘079 patent was previously involved in the following court proceeding identified by Petitioner: *Textile Computer Systems, Inc. v. Fort Worth City Credit Union*, Case No. 2:16-cv-01048 (E.D. Tex.).

III. THE ‘079 PATENT AND PRIOR ART

A. The ‘079 Patent

The ‘079 patent introduced a robust and versatile authentication system for giving temporary, limited and transaction specific access to secured resources to specific individuals and entities that is reliable and readily accessible to virtually any application.

The ‘079 patent teaches a transaction protocol that involves four parties: an authorized user (*e.g.* consumer), an unauthorized service client (*e.g.*

merchant), a service provider (authenticator) and a resource provider (*e.g.* credit card processor) as shown in FIGS 1-4. "The service client 33 of the present invention will generally provide for an end user actor 34 a means 37 for submitting an authentication credential to the service client 33 for use by the service client 33 in obtaining from the service provider 36 access to the requested secured resource." EX1001 at 4:24 - 4:29; Oglesby Decl. at ¶¶ 15-16.

As shown in FIGS 1-4, the ‘079 patent system authenticates the identity of a requester of access by an unauthorized service client to a secured resource. In the ‘079 patent the authorized user has the right to normal use of the secured resource (such as their social security or credit number) requests access to that secured resource by someone who does not otherwise high the normal right to use the resource (such as merchant who wants payment from the credit card account).

As particularly shown in FIGS. 2 and 4, the authentication method 46 generally begins with an unauthorized service client 33 (*e.g.* merchant) providing identification and transaction specific data to the authorized service client 34 (*e.g.* consumer a/k/a "authorized user") which the latter uses to generate a transaction specific request message which is transmitted to a messaging gateway 60 of service provider 36. The request message from the authorized service client 34 informs the service provider that the authorized service client wishes to provide access to a selected secured resource to a specific service client 33 for a specific transaction. EX1001 5:24 - 5:49; Oglesby Decl. at ¶¶ 17-18.

When the service provider 36 receives the request, a transaction entry is created in a transaction database with the transaction details and the identifier of the resource which maps to the common identifier for the resource known by the resource provider 43 necessary to provide access to the resource. Thus, by not saving the primary account number of bank accounts or credit cards, the possibility of the service provider 36 (*i.e.* authenticator) also being hacked for this information, or themselves engaging in credit card fraud, is eliminated in an implementation where the service provider 36 is a different entity than the resource provider 43 (*e.g.* issuing bank).

When the end user 34 has multiple secured resources the access to which is being managed by the service provider 36, both the service provider 36 and the end user 34 will also know a pseudonym for each resource so that the user can include the pseudonym in the request so the proper resource identifier can be recorded in the transaction database.

In particular, a transaction entry is created in a transaction database with the transaction details including the identifier of the unauthorized user and resource identifier, which in turn maps to the common identifier for the secured resource known by the resource provider 43 and necessary to provide access thereto. For further security, the '079 patent teaches using pseudonyms to identify which secured resource the authorized user wishes to be used for the transaction when communicating with the service provider. (EX1001 3:53-67; 3:60-67; 14:3-4:60). Thus, when the authorized user has multiple secured resources to which access is being managed by the service provider 36, both the service provider 36 and the end user 34 will know a pseudonym for each resource so that the user can include the pseudonym in the request so the proper resource identifier can be recorded in the transaction database. Oglesby Decl. at ¶ 19.

The request also results in a transaction specific key string being generated which the consumer passes to the merchant to use as an authentication credential. The unauthorized service client in turn forwards the authentication credential, along with additional input, to the service provider. The authentication credential is used to authenticate the identity of the requester as the authorized user. “To complete the transaction, the consumer will indicate a desire to make a payment to the [merchant] by submitting to a service provider 36 a request for payment to the service client 33 and for authentication of the consumer’s right of access to an identified secured payment resource, whereafter the end user 34 will provide a previously established authentication credential to the service client 33. The service client 33 will then forward the authentication credential to the service provider 36 for validation in order to obtain payment from the identified secured payment resource as requested by the consumer.” EX1001 at 10:18-28 The user's request will contain data obtained from the merchant that generally will include a merchant identifier and transaction details. EX1001 at 10:37-11:47; 12:50-57; 14:3-15:28; 15:67–16:15; 16:29-16:40; Oglesby Decl. at ¶ 20.

When the authentication credential is submitted by the unauthorized service client to the service provider, the unauthorized service client also submits its identifier in the request so that it may be compared with the corresponding identifier submitted with the authorized user's access request. The authentication credential will be used by the service provider to look up the associated information submitted by the authorized user to see whether this information matches the input provided by the merchant (*i.e.* the merchant identifier etc.) for the transaction. *See* EX1001 at 5: 24 – 49 and 12: 50 – 57 (end user submits a Request Message designating a specific service client and identifies a specific secured resource to be used in completing the transaction); EX1001 at 13: 46 – 61 (user submitted merchant identifier associated with authentication credential compared with merchant submitted identifier to authenticate the identity of the authorized user as originator of the request.)

The system thus evaluates the authentication credential, for example in a credit card transaction with a merchant, by comparing the merchant identifier submitted by the credit card holder with the merchant identifier submitted by the unauthorized service client by using the authentication credential to look up the associated merchant identifier submitted in the authorized user's request. Only if there is a match will the identity of the authorized user be authenticated as having approved the transaction. Oglesby Decl. at ¶ 21-22.

"With the authentication credential found to be correct, the service provider 36 may simply report the correct finding to the service client 33 or, if for security or other reasons the service client 33 is unable to directly access features or functionality of a resource for which an end user actor 34 has requested access, the service provider 36 will then obtain for the end user 34 and/or the service client 33 the benefit of the requested secured resource and thereafter appropriately report the conducted transaction to the service client 33 and/ or the end user 34." (EX1004 7:4 – 7:13; 16:41 - 16:45) ("If the request handler 51 determines that a resource should be accessed, a resource request is formulated using the transaction parameters stored in the transaction database 59 and any additional information as may be necessary that is stored in the user database 58.") Thus, upon successful authentication of the authorized user's identity, the service provider will retrieve the common identifier for the resource and submit it to the resource provider for normal processing. Oglesby Decl. at ¶ 23.

"In <u>a critical aspect</u> of the authentication system 30 and method 46 of the present invention, an additional security measure is implemented by <u>requiring</u> that the service client 33 be restricted from access to the common identifier for the secured resource, e. g. the account number for a credit card or financial deposit account; the Social Security Number of a patient; the account number of an ATM card; or the like." (EX1001 at 8:4 – 8:10) "In accordance with a <u>critical aspect</u> of the present invention, however, the automobile fueling station, restaurant or on-line retailer c<u>annot be provided with or otherwise be made aware of either the consumer's credit card or checking account number and also must not be given any information that would allow the automobile fueling station, restaurant or on-line retailer to repeat the transaction without again obtaining authorization from the consumer</u>." (EX1001 10:29 - 10:36) (emphasis supplied). Thus, neither the key string nor the authentication credential therefore reveal the common identifier, such as the primary account number ("PAN"), of the resource to which is access is being given to the unauthorized service client or any information that would again allow the unauthorized service client access to the secured resource without the authorized user again giving permission. Moreover, the authentication credential is used to authenticate the requester's identity in determining whether to provide the third-party access to the authorized user's secured resource. Oglesby Decl. at ¶¶ 24-25.

Again, only if the merchant identifiers respectively submitted by the user and the merchant match will the system identify the authorized user as the originator of the request and proceed with the transaction. The '079 not only allows credit card transactions to take place through normal processing without having to give the merchant the credit card number, but also prevents any credit card transactions from taking place that were not authorized by the user. Thus the system only allows a transaction to take place for a specific merchant designated by the user to use a specific credit card number designated by the user, preferably for a specific amount and within a specific time period. See EX1001 at 5: 24 – 49 and 12: 50 – 57 (end user submits a Request Message designating a specific service client and identifies a specific secured resource to be used in completing the transaction); (user submitted merchant identifier associated with authentication credential compared with merchant submitted identifier to authenticate the identity of the authorized user as originator of the request.) Oglesby Decl. at ¶¶ 26.

With this in mind, the end user 34 may, for example and without limitation, be a patient wishing to share medical information (a secured resource) with a healthcare or medical insurance provider (a service client 33) without having to grant to the healthcare or medical insurance provider unfettered access to all of his or her medical records; the end user 34 may be the holder of a credit card account, banking account, automated teller machine ("ATM") card and/or account or the like (a secured resource) wishing to purchase merchandise, services, information or the like from a retail store, service station, on-line service provider or merchandiser, other business or the like (a service client 33) without providing the service client 33 with his or her full credit card information, e. g. without providing his or her Card Verification ("CV") code, banking account information, personal identification number ("PIN") associated with the ATM card or the like; or a credit applicant or other holder of an information product wishing to share a credit score or other information (a secured resource) with a consumer of information products, such as an automobile dealership in need of consumer credit data or the like (a service client 33) without providing his or her Social Security Number or other information not necessary to the conduct of the present transaction. EX1001 at 7:47–8:3; Oglesby Decl. at ¶ 27.

Again, the '079 system thus not only allows credit card transactions to take place through normal processing downstream of the merchant without having to give the merchant the credit card number, but also prevents any credit card transactions from taking place that were not authorized by the user, by having the authenticator inject the credit card number into normal processing downstream of the merchant. Oglesby Decl. at ¶ 28.

In sum, the '079 patent's payment system uses a four-party transaction protocol between a service client, end-user, service provider and a resource provider enabling temporary access to an authorized user's secured resource. In the context of a credit card transaction, a real-time payment request from the consumer (at a point-of-sale location) results in the local generation of a key string by the consumer's device. The key string does not represent an account number, rather it provides consumer authentication plus a set of instructions through which the specified transaction may be completed. The consumer's device provides the key string to the merchant's device for forwarding by the merchant's device to the service provider's server. The service provider server uses the key string to verify the request is authorized by the consumer. Upon authentication, the service provider server looks up the payment instructions associated with that key string, including the designated secured resource (the credit card credentials), and passes them to the merchant's payment processor's system or collection of funds from the selected credit card account. Oglesby Decl. at ¶ 29.

B. Johnson

Johnson is directed to on-line transactions in which the merchant does not wish to trust payment from the buyer but is willing to accept payment through a payment provider. Johnson teaches an online guaranteed payment system using a three-party double payment transaction protocol wherein the buyer pays a payment provider for a payment token, presents the payment token to the merchant, and the merchant is subsequently paid from the payment provider upon presentation of the token. A POSITA reading Johnson would understand it to follow the old certified check (a/k/a bank demand draft (DD)) model modified for on-line use.[2] Oglesby Decl. at ¶ 30.

In Johnson, the three parties are the merchant, consumer, and a payment provider and two payment transactions are required. In the first payment transaction, the payment provider transfers funds from consumer's account to the payment provider account to fund the payment to the merchant. Subsequently, in a second payment transaction, the payment provider transfers the funds to the merchant upon presentment of a payment token. Johnson's payment token is thus like a certified check where the payment provider and consumer pre-reserve funds for the merchant's subsequent withdrawal and the merchant can "cash" the payment token later with the assurance the funds are held by the payment provider. Oglesby Decl. at ¶ 31.

[2] A Bank Demand Draft (e.g. Certified Check) is "…a negotiable instrument similar to a bill of exchange. A bank issues a demand draft to a client (drawer), directing another bank (drawee) or one of its own branches to pay a certain sum to the specified party (payee)." https://en.wikipedia.org/wiki/Demand_draft. In a commercial setting, the merchant and buyer have a purchase order, the purchaser (drawer) makes the payment of the amount of the purchase order to a financial institution (bank) and requests the bank to issue a demand draft for that amount with the merchant as payee. Because payment of the demand draft is guaranteed by the bank, the merchant is willing to receive the demand draft in lieu of payment from buyer and can therefore release the goods to the buyer upon receipt of the demand draft. Upon presentation of the demand draft, the merchant has the amount of the demand draft transferred from an account at the bank holding the pre-paid funds to cover the transaction into their own account through the bank's clearinghouse.

As Johnson describes, the consumer buys the payment token from a given payment provider selected by the user. (EX1004 at [0052]) **<u>(“To obtain a payment token</u>**, it may be necessary to first establish an identity via an identity token, as described in further detail below. In either case, end-user 110 may…”) (EX1004 at [0100]) (**<u>“Based on the user input 1040, the appropriate payment provider 1005 may be contacted for proper funding</u>** of the services and/or goods.”); (EX1004 at [0042]) (“Such payment tokens **<u>offer proof </u>**of the consumer’s ability to pay for the service and/ or goods by allowing the merchant to validate the authenticity of the token directly with the payment provider.”) The payment provider will not issue the payment token unless “the end-user payment information is correct, sufficient funds are available, and/or the payment provider otherwise certifies that it will pay on the end-user's behalf.” (EX1004 at [0065])

Johnson’s payment token acts as “verification of a user's ability to pay for the purchase.” (EX1004 at [0013]); also at [0042] (“Such payment tokens offer proof of the consumer’s ability to pay for the service and/ or goods by allowing the merchant to validate the authenticity of the token directly with the payment provider.”) A POSITA would understand the payment token is used by the merchant to access the reserved funds, over which the buyer does not have ordinary use or control. The payment token also does not meet the limitation of a key string under the ‘079 patent because the token could be the certified check number (or an encrypted form of that number) or other common identifier for the account to be used to pay the merchant. Regardless of whether or what secured information may be associated with the payment token, this is not the buyer's secured resource. Moreover, the payment token is not used in a request to access the buyer's account, rather it is used to access the reserved funds. Oglesby Decl. at ¶¶ 32-33.

In Johnson, the user must contact a payment provider to arrange the funding for the purchase of a payment token and use that payment token to pay for the transaction. In this manner, Johnson is analogous to paying for a car wash token and then using the car wash token to get your car washed. Oglesby Decl. at ¶¶ 34.

C. Stambaugh

Similar to Johnson's system, Stambaugh implements an SMS based three-party double transaction protocol using a merchant specific (*i.e.*, "closed-loop") prepaid account that is under the control of a payment authority. The prepaid account is funded in advance from a consumer's financial account and the available funds may be spent only at the designated merchant(s). The user enrolls with each merchant that they choose to pay through Stambaugh's system.

In essence, Stambaugh is directed to an on-line merchant loyalty program in which, like Johnson, the confirmation code acts as a pre-paid payment token which may be used at the designated merchant and submitted for payment. Thus, an entity manages the prepaid account funded from consumers' financial account (example: credit card, bank account and the like) that is used to pay the merchant. Thus, the consumer's financial account is first used to pay the payment authority to fund a balance that will be consumed over time through the issuance of multiple payment tokens (*i.e.*, confirmation codes) that are spent at the designated merchants. (EX1005 at 7:19 – 7:37); Oglesby Decl. at ¶ 35.

A POSITA would also understand such systems have costs not associated with direct payment transactions. For example, for the consumer, interest would accumulate while funds are held in financial accounts, but not when the funds are held in a merchant-designated prepaid account. Therefore, consumers will incur opportunity cost for the balances left in the prepaid account. Such systems often also result in consumers losing valuable warranty, return policy extensions, price protections and other benefits that come from making a payment directly with their credit cards. Oglesby Decl. at ¶ 36.

In sum, Stambaugh teaches a payment authority that controls, maintains and holds the funds deposited in the prepaid account having a periodic recharge option. Like Johnson, Stambaugh also uses a three-party double payment protocol wherein the user, payment authority and merchant are the three parties and the first payment transaction is to transfer funds from user's financial account to the user's prepaid account with the payment authority and the second payment transaction is to transfer funds from the prepaid account to the merchant's financial account. The transaction code used by Stambaugh is used to make a payment from the payment authority like an on-line gift card or stored value card. Oglesby Decl. at ¶¶ 37.

D. Sellars

Sellars is in the field of distribution of content in relationship to payment processing. (EX1006 [0002]). ("Embodiments of the invention relate to the distribution of content (such as text, audio, video, multi-media materials, and the like). More particularly, the invention relates to the distribution of such content in a manner that ensures that the copyrights and other similar legal rights of the content owner are respected.")

Sellars is directed to encryption and decryption of data in which transaction data is first encrypted (to prevent its access by the merchant, for example) for transmission to a decryption device where the data is then decrypted and used to generate a payment request. The payment request is then encrypted for transmission to a second decryption device for decryption. (EX1006 at Abstract). Common account identifiers are thus kept confidential through encryption (in some cases of a secret account identifier) and payment authorizations "are encrypted with a mutating ID" (EX1006 at [0225]); Oglesby

Decl. at ¶¶ 38-39.

Like Johnson, Sellars teaches a protocol for online commerce transactions (whereas 079 supports all types of transactions.). An exemplary embodiment of the protocol involves the four participants discussed above. The entity Bob ("B") performs the role of the buyer 260, the entity Vera ("V") performs the role of the vendor 220, the entity Carol ("C") performs the role of the payment authenticator 240, and the entity Trent ("T") performs the role of the authenticator 280. (EX1006 at [0229]). It does not disclose a system or method like the ‘079 patent wherein the authorized user (e.g. consumer) requests access for an unauthorized service client (e.g. a specific merchant) to a specified secured resource (e.g. a given credit card number designated by the consumer to be used to process the transaction) in which a one-time key string associated with the transaction known is used to make an authentication credential passed by the authorized user to the unauthorized service client to be provided, along with additional input from the unauthorized service client to the service provider, to authenticate the identity of the authorized user as the requester. Oglesby Decl. at ¶ 40.

IV. CLAIM CONSTRUCTION

A. Level of Skill of a Person Having Ordinary Skill In The Art

A person of ordinary skill in the art of the ‘079 Patent at the time of the claimed invention **(“POSITA”)** would have been a person having the equivalent of either a business degree (e.g., a bachelor's in business, economics, finance or similar discipline) or a degree in computing (e.g., a bachelor's in computer science, electrical engineering, or similar discipline), with at least two years of experience in designing and deploying electronic payment and security systems in order to be capable of understanding the '079 patent and the prior art references discussed herein. Oglesby Decl. at ¶¶ 41.

B. Broadest Reasonable Interpretation

A claim subject to *inter partes* review receives the "broadest reasonable construction in light of the specification of the patent in which it appears." 42 § 42.100(b); *see Cuozzo Speed Technologies, LLC v. Lee,* 579 U.S.___(slip op. June 20, 2016); 2016 WL 3369425. In some circumstances, the broadest reasonable interpretation (BRI) standard should yield a construction that is in all essential respects identical to the construction that the courts would apply after engaging in the Federal Circuit guided *Markman* procedure. In *Microsoft Corp. v. Proxyconn, Inc.*, 789 F. 3d 1292, 1298 (Fed. Cir. 2015), the court explained that the BRI standard does not give the Board authority to reach an interpretation divorced from the specification and file history:

> "That is not to say, however, that the Board may construe claims during IPR so broadly that its constructions are *unreasonable* under general claim construction principles. As we have explained in other contexts, "[t]he protocol of giving claims their broadest reasonable interpretation . . . does not include giving claims a legally incorrect interpretation."

In re Skvorecz, 580 F.3d 1262, 1267 (Fed. Cir. 2009); *see also In re Suitco Surface, Inc.*, 603 F.3d 1255, 1260 (Fed. Cir. 2010) ("The broadest construction rubric coupled with the term 'comprising' does not give the PTO an unfettered license to interpret claims to embrace anything remotely related to the claimed invention."). Rather, "claims should always be read in light of the specification and teachings in the underlying patent." *Suitco*, 603 F.3d at 1260. The PTO should also consult the patent's prosecution history in proceedings in which the patent has been brought back to the agency for a second review. *See Tempo Lighting Inc. v. Tivoli LLC*, 742 F.3d 973, 977 (Fed. Cir. 2014). Even under the broadest reasonable interpretation, the Board's construction "cannot be divorced from the specification and the record evidence," *In re NTP, Inc.*, 654 F.3d 1279, 1288 (Fed. Cir. 2011), and "must be consistent with the one that those skilled in the art would reach," *In re Cortright*, 165 F.3d 1353, 1358 (Fed. Cir. 1999). A construction that is "unreasonably broad" and which does not "reasonably reflect the plain language and disclosure" will not pass muster. *Suitco*, 603 F.3d at 1260. *Id.* at 1298.

To arrive at the legally correct construction, the PTAB must consider the patent and file history as a whole to determine meaning, even in cases where the dictionary definition of the claim term might lead one to a broader interpretation. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1317 (Fed. Cir. 2005) (en banc). Indeed, the Federal Circuit has often stated that claim construction is the process of determining "the reasonable" construction of the claim. Surely, those cases cannot be interpreted as accepting only one of a wide range of possible constructions. *See In re Suitco Surface, Inc.*, 603 F.3d 1255, 1260 (Fed Cir. 2010); *In re Skvorecz*, 580 F.3d 1262, 1267 (Fed. Cir. 2009); *In re NTP, Inc.*, 654 F.3d 1279, 1288 (Fed. Cir. 2011).

With the extensive tools provided to the PTO and the lower courts, the governing case law provides the appropriate method for determining the "true meaning of language used in the patent claims." *Phillips*, 415 F. 3d at 1318. Claims must be construed as a whole; the context of the claim often provides convincing evidence of the meaning of terms within the claim. *Id*. at 1313 ("Importantly, the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification.").

The Federal Circuit recently reiterated and reinforced these restrictions on the PTAB's authority to construe terms under its BRI standard in a far different manner than a district court would in patent infringement litigation. In *Straight Path IP Group, Inc. v. Sipnet EU S.R.O.*, 806 F.3d 1356 (Fed. Cir. 2015), the Federal Circuit overturned a finding of invalidity on the basis that the Board had improperly broadened the "plain" reading of the claim by reference to material in the specification: "For that reason, the court has repeatedly stated since *Phillips* that redefinition or disavowal is required where claim language is plain, lacking a range of possible ordinary meanings in context. *See Pacing Technologies, LLC v. Garmin Int'l, Inc.*, 778 F.3d 1021, 1024 (Fed. Cir. 2015) (citing authorities)."

C. Petitioner's Proposed Constructions are not Reasonable or are Entirely Missing.

Petitioner has offered constructions of terms from the patent claims which are not the "broadest reasonable interpretations" of the terms. Nonetheless, only four (4) issues of claim construction must be resolved in order to deny institution of a proceeding here. Those issues are how the following terms should be interpreted: (1) "authorized user of a secured resource"; (2) "unauthorized service client"; and (3) "key string"/"authentication credential"; and (4) messaging gateway.[3] In construing these terms, the Board must be careful to apply an interpretation that is consistent with the context of the particular claim in which the term appears "(including surrounding claim language) and in the context of the specification of the ['079] Patent." *Nike, Inc. v. Adidas AG,* 812 F.3d 1326, 1346 (Fed. Cir. 2016).

1. "Authorized User of a Secured Resource"

[3] This term does not require construction to resolve the matters raised by the Petition. However, because Petitioner has supplied a construction narrower than required by the specification, Patent Owner submits the proper broadest reasonable construction for the record. The Board should only construe those terms germane to determine the validity of the claims.

This claim term is included in each independent claim of the '079 patent and broadly means "the user having the right to control access to the secured resource." Oglesby Decl. at ¶ 42.

The specification reflects the authorized user of the secured resource is the entity having the right to control access to the secured resource, such as a credit card holder who can control access to the corresponding credit card number and account, or the person whose medical file access is being provided. EX1001 7:14 – 7:46 ("Under the present invention, a service provider 36 having associated therewith a hardware and/or software implementation of the previously generally discussed functionality is in accordance with the present invention programmed or otherwise adapted to receive directly from the service client 33 an end user provided authentication credential associated with the service client 33 as a result of a request by the end user 34 for the service provider 36 to provide for the service client 33 access to a secured resource and, thereafter, to validate the authentication credential from the service client 33 to ensure that the request is made under the authorization of an end user 34 having right of access to the secured resource.")

The specification is equally clear that the authorized user had the right to control other's access to the secured resource. ("With this in mind, the end user 34 may, for example and without limitation, be a patient wishing to share medical information (a secured resource) with a healthcare or medical insurance provider (a service client 33) without having to grant to the healthcare or medical insurance provider unfettered access to all of his or her medical records; the end user 34 may be the holder of a credit card account, banking account, automated teller machine ("ATM") card and/or account or the like (a secured resource) wishing to purchase merchandise, services, information or the like from a retail store, service station, on-line service provider or merchandiser, other business or the like (a service client 33) without providing the service client 33 with his or her full credit card information, e.g. without providing his or her Card Verification ("CV") code, banking account information, personal identification number ("PIN") associated with the ATM card or the like… (EX1001 at 7:47-7:67)

Thus, this construction is broadly consistent with the plain meaning of the claim language in light of the specification. Oglesby Decl. at ¶¶ 43-45.

2. "**Unauthorized Service Client**"

The '079 patent restricts the service client 33 from the knowledge needed for ordinary full use of the secured resources. EX1001 at 7:14 – 7:46 ("access for the service client 33 to a secured resource for which the service client 33 is restricted from full knowledge and for which the service provider 36 may hold full knowledge, full knowledge being defined herein as knowledge sufficient to make ordinary full use of the secured resource…"). The resource may comprise password protected information (e.g., a credit report) a portion of which (e.g., only the credit scores) a human end user 34 wishes to share with a service client 33 comprising an information consumer (e.g., a potential creditor) without providing to the information consumer the password (e.g., by which the full credit report is protected and as would otherwise enable the potential creditor to gain full access to the protected credit file) or it may be "the account number for a credit card or financial deposit account; the Social Security Number of a patient; the account number of an ATM card; or the like." (EX1001 at 8:4 – 8:10).

The specification is equally clear that "[i]n a critical aspect of the authentication system 30 and method 46 of the present invention, an additional security measure is implemented by requiring that the service client 33 be restricted from access to the common identifier for the secured resource, e. g. the account number for a credit card or financial deposit account; the Social Security Number of a patient; the account number of an ATM card; or the like." (EX1001 at 8:4 – 8:10). "In a critical aspect of the authentication system 30 and method 46 of the present invention, an additional security measure is implemented by requiring that the service client 33 be restricted from access to the common identifier for the secured resource, e. g. the account number for a credit card or financial deposit account; the Social Security Number of a patient; the account number of an ATM card; or the like." (EX1001 at 7:46-8:10) "In accordance with a critical aspect of the present invention, however, the automobile fueling station, restaurant or on-line retailer cannot be provided with or otherwise be made aware of either the consumer's credit card or checking account number and also must not be given any information that would allow the automobile fueling station, restaurant or on-line retailer to repeat the transaction without again obtaining authorization from the consumer." (EX1001 at 10:9 - 10:36).

Therefore, the term broadly means in light of the specification "a service client that is unable to make ordinary full use of the secured resource without further permission from the authorized user." Oglesby Decl. at ¶¶ 46-48.

3. "**String**"

The '079 patent teaches that a ""string" shall for purposes of the present invention be expressly defined to mean "an ordered sequence of any subset of symbols selected from a set of symbols wherein each symbol forming the set may be represented in both a format that may be perceived by an end user 34 and a format that may be recognized by software or hardware," e.g. the set of all alphabetic and numeric characters in the English language. Although not strictly necessary for the conduct of the present invention, it will be desirable, in at least those implementations requiring human handling of an authentication credential, that the authentication credential comprise symbols that also may be perceived by a human end user 34." (EX1001 at 15:29 – 15:40).

So, the broadest reasonable interpretation of "string" is an ordered sequence of symbols. Oglesby Decl. at ¶¶ 49-50.

4. "Key String/Authentication Credential"

The '079 patent's teachings include "determining a key string adapted to provide a basis for authenticating the identity of the requester" where the key string is known to both the service provider 36 and the end user 34 and which is used by end user 34 to pass an authentication credential in connection with the transaction in progress to the unauthorized service client. (EX1001 at 6:49 – 6:55). An exemplary way to determine the key string to be adapted as an authentication credential to access a secured resource is described at 13:58 – 15:25 using user and transaction databases. See also FIGS. 7, 8.

The specification excludes as a key string any information sufficient to make ordinary full use of the secured resource outside of the framework of the authentication system and expressly excludes the key string being a common identifier for the secured resource to which access is being provided, such as the account number for a credit card or financial deposit account. (EX1001 at 2:27 – 2:38; 7:14 - 8:10). Furthermore, the key string cannot provide any information that would allow the unauthorized user to repeat the transaction without again obtaining authorization from the authorized user. "In accordance with a critical aspect of the present invention, however, the automobile fueling station, restaurant or on-line retailer cannot be provided with or otherwise be made aware of either the consumer's credit card or checking account number and also must not be given any information that would allow the automobile fueling station, restaurant or on-line retailer to repeat the transaction without again obtaining authorization from the consumer." (EX1001 at 10:9 - 10:36).

Therefore, the broadest reasonable interpretation of "key string" is: the string used to create an authentication credential that does not reveal the common identifier of the secured resource, such as the bank account or credit card number, or any other information that would allow the unauthorized service client to gain access the secured resource without again obtaining authorization from the authorized user." Oglesby Decl. at ¶¶ 51-53.

5. "Messaging Gateway"

The messaging gateway 60 is used for bi-directional transfer of messages between user applications running on external devices and the application server 50. See description of forms of bi-directional transfer of messages from the authorized user and unauthorized service client and the application server at (EX1001 at 11:54 – 11:63); (EX1001 at 12:9 – 12:64). The messaging gateway is "preferably [a] unified messaging gateway" for use "through various communication channels." (EX1001 at 9:32-9:55).

As the ‘079 patent explains, such a unified messaging gateway 60 may be utilized to receive a request message 84 or transmit a generated confirmation message 94 in any of a plurality of message formats for a plurality of communication channel such as, for example, an SMS or other text channel, a simple mail transport protocol ("SMTP") channel, a plain old telephone system ("POTS") channel, a paging network or private broadcast channel or the like to be received by any of a plurality of user devices. EX1001 at 9:32-50. Based on the description given in the ‘079 patent, a POSITA would understand that the messaging gateway would typically be implemented via a software platform for bi-directional transfer of messages between external source devices and the service providers’ application servers.

Thus, the broadest reasonable interpretation of “messaging gateway” should be “a platform for bi-directional transfer of messages between user applications running on external devices and an application server.” Oglesby Decl. at ¶¶ 54-56.

Petitioner asserts the “messaging gateway” is “a device for use in transferring messages between a plurality of communications channels by converting messages between a plurality of message formats.”

This is not the broadest reasonable interpretation because it reads into the term capabilities which are explicitly stated in the ‘079 to only be preferred, and not necessary. However, it is not necessary to interpret this term for the purposes of resolving the Petition. Oglesby Decl. at ¶¶ 57-58.

V. THE COMBINATION OF JOHNSON & STAMBAUGH CANNOT RENDER OBVIOUS CLAIMS 1, 3, 6-9, 11, 13, AND 16-19 OF '079 PATENT (GROUND 1)

A. Johnson Does Not Meet Independent Claims 1 & 11

The combination asserted by Petitioner in Ground 1 does not render obvious any claims of the '079 because the asserted combination does not teach all of the elements of any claim nor would a POSITA be motived to add the message authority of Stambaugh to Johnson's system.

Petitioner asserts the '079 patent to simply use "dummy key strings (or tokens) rather than sensitive account numbers in the clear." Pet at 1. This is incorrect. The '079 uses authentication credential which has the specific necessary characteristics and functions in the system. Neither Johnson nor Petitioner explain how "dummy" key strings or tokens are generated or show these to have the necessary characteristics and functions as in the '079 patent discussed above.

Petitioner also incorrectly asserts Johnson discloses the '079 protocol. Johnson automates a previously manual and paper-based process for on-line use. It is a digital version of the old certified check system to guarantee payment for goods or services ordered on-line, in which funds are transferred from consumer's financial account to a payment provider's financial account and a token is provided to assure payment from the payment provider financial account to the merchant financial account.

A POSITA would understand Johnson is similar to a certified check created for on-line purchases because:

- Johnson states "a payment token will not be issued unless the end-user payment information is correct, sufficient funds are available, and/or the payment provider otherwise certifies that it will pay on the end-user's behalf" - this means that the issuer of the token is the same party as the party that will fund the payment.
- Johnson also states that "the payment token operates as assurance" several times (particularly in [0066]). The linkage between the words "token" and "assurance" means that the token is backed financially by the issuer of the token. Therefore the issuer of the token must pay the merchant upon redemption of the token.
- [0067] - states the transaction is "substantially risk free"
- Johnson also states that the payment token may be processed without authorization. ([0062] states that "the merchant may treat the payment token essentially as payment", and Fig 3 specifically states that service provider validation of the payment token is

optional.)

This is a digital version of a certified check. A certified check is backed financially by the issuing organization, and it requires no authorization/validation from the recipient. It can be treated essentially as payment. Oglesby Decl. at ¶¶ 59-63.

In contrast, the ‘079 teaches a method in which a secured resource (e.g. the user’s credit card number) can be selected from several available resources and then accessed by the system to complete a specific transaction for a given unauthorized service client. The ‘079 can be used at online or physical retail locations, including, pay at the pump, ATM and over the phone etc. For credit card transactions, the ‘079 technology allows the user to ensure no unauthorized credit card transactions take place and use any credit card account at any merchant without having to present in any manner the credit card number. None of the complicated limitations of Johnson are present in the ‘079 because the ‘079 is not limited to any specific payment provider. Indeed, in the ‘079, the service provider only needs to validate the authentication credential and the associated secured resource of the authorized user (e.g. credit card number assigned for the transaction) will then be normally processed downstream of the service provider to process the payment transaction from the consumer’s financial account to the merchant’s financial account. Oglesby Decl. at ¶ 64.

The ‘079 focuses on providing access to a "secure resource”, and it is clear that the “secure resource” is not the live PAN nor can one authorization credential provide any more than one-time access to the use of a PAN. This is another key difference. In Mott’s view, a token represents a PAN. In ‘079, the key string specifically does not represent a PAN. In ‘079, the key string represents:

- The authorized user whose secure resource is to be accessed in completing the transaction so the user remains anonymous to the service client/merchant but when the service provider receives the key string/authentication credential it immediately knows the identification of the authorized user/consumer); and
- The consumer’s payment instructions (who is permitted to use the token/key string (restrictions by merchant), when is the merchant allowed to use the token/key string (time limitations), how much is to be paid (can be a specific amount or an up-to limit), which of several PANs are to be utilized to complete the transaction (could be instructions to use a single account or instructions to split the bill between multiple accounts)). So, in Johnson/Mott a token=an account number that has been disguised. See ¶¶ 37-38 of Mott’s declaration where Mott asserts that ‘079 patent authentication token merely represents a disguised account number. This is incorrect. In

> the ‘079 patent, the authentication credential represents a set of instructions that will result in a completed transaction but it is not in any way a disguised account number.

Johnson provides an on-line system which automates the old manual system of providing guaranteed payments, such as certified checks, in order to secure the release of the goods/services from the merchant. It is not directed to securing sensitive information, such as a credit card number, that is needed to be accessed in processing a normal payment transaction from the buyer’s financial account to the merchant’s financial account, such as the ‘079. Oglesby Decl. at ¶¶ 65-66.

Indeed, Johnson’s payment token is the only information necessary for Johnson’s system to make the guaranteed payment from the payment provider to the merchant, and it is freely given to both the merchant and the buyer. In other words, Johnson does not process a credit card transaction from the buyer to the merchant. Instead, the buyer buys a token from the payment provider and presents the payment token to the merchant (instead of a certified check.) The merchant can then confidently release the goods and services without first receiving payment because the payment token indicates to the merchant that the funds are guaranteed to come from the trusted payment provider.

In contrast, in a credit card transaction, merchants must seek authorization for the payment before releasing the goods/services because there is no payment guarantee.

Johnson's field of endeavor is thus to computerize or automate an existing manual process where a merchant can conduct an online commercial transaction using a specific payment provider who will obtain the funds for the transaction from the byer and hold funds in a financial account for the merchant for payment to the merchant upon presentation of the payment token (three-party double payment transaction protocol.) Oglesby Decl. at ¶¶ 67-69.

The '079 patent's field of endeavor is to identify and verify authorization to use secured resources in third party transaction while protecting the common identifiers of the secured resources, readily usable in virtually any application and economical in implementation using a four-party single payment transaction protocol. Therefore, Johnson is not analogous to the claimed invention of the '079 patent and is not in the same field of endeavor.

Stambaugh is in the same field of endeavor as Johnson because it also uses a three-party double payment transaction protocol wherein a text or SMS message or email communication channel is used to receive a non-merchant specific code to pay for services and/or goods from a rechargeable prepaid account. Therefore, Stambaugh is likewise not also not in the same field of endeavor or analogous to the claimed invention of the '079 patent, which does not require payment be made through pre-paid funds held by specific payment authorities. Oglesby Decl. at ¶¶ 70-71.

Stambaugh creates a digital version of a merchant-branded gift/prepaid card while Johnson is creating a digital certified check. They are similar in nature except that a prepaid account is a carried balance used to fund multiple transactions in Stambaugh whereas Johnson has no balance carryover. The '079 does not contemplate managing balances at all nor does it require any special arrangement between merchant and consumer. Oglesby Decl. at ¶ 72.

Stambaugh may be seeking to provide wireless payment transaction system utilizing multifactor authentication, but very differently than as used by '079. In the first place, when Stambaugh's payment authority receives the transaction code from the transaction authority (step 602), the payment authority will merely recognize the complete code as a valid code and approve the transaction regardless of who is requesting the funds. EX1001 at 8:19 – 8:30. Thus the transaction code may be misused if it falls into the wrong hands. The '079's authentication code, in contrast, is worthless in the wrong hands because it is specific to an individual transaction. EX1001 at 11:29 - 11:37; 12:50 - 12:57; Oglesby Decl. at ¶ 73.

The wireless payment transaction system utilizing a multifactor sought by Stambaugh is not same as the one sought by '079. Oglesby Decl. at ¶ 74.

B. <u>Johnson's Token Request is Not a "Request For Access By An Unauthorized Service Client to Said Secured Resource"</u>

Johnson's payment token request does not constitute "request for access by an unauthorized service client to said secured resource" of the '079 patent, because the purpose, content and content usage between Johnson teachings and '079 teachings are much different.

Johnson's payment token is not a secured resource of the authorized user nor does it provide access to a secured resource of the authorized user. The buyer in Johnson is not buying a payment token to provide access to a secured resource of the buyer (such as the buyer's credit card account). Rather, the buyer shares the payment token with the merchant to confirm the payment provider holds the funds to pay the merchant for the transaction upon presentation of the token. The merchant subsequently presents the payment token to the payment provider to receive the payment from the payment provider that was funded by the buyer in obtaining the payment token.[4] Johnson's system thus provides access to the merchant to funds reserved at the payment provider for the merchant. The

[4] In '079 the service provider may generate a receipt to the authorized user because there is real-time, electronic communication between the merchant and the service provider and there is an authorization/confirmation of the payment. As such, the service provider may collect detailed information about the purchase, and confirm payment has been made including that detailed information. This is not the case when a certified check and/or Johnson's teachings are involved, because there is no electronic exchange of information between the payer and the payee, nor is there an intermediary that is collecting the information needed to generate the receipt.

authorized user does not control those funds. Oglesby Decl. at ¶¶ 75-76.

Based on the above facts, a POSITA would conclude that Johnson's payment token request does not constitute the claimed "request for access by an unauthorized service client to said secured resource" that is received "from a requester purporting to be an authorized user of a secured resource." Oglesby Decl. at ¶ 77.

C. **Johnson's Server Does Not "Determine A Key String Known To Both Said Secured Resource And The Authorized User Said Requestor Purports To Be, Said Key String Being Adapted To Provide A Basis For Authenticating The Identity Of Said Requester"**

Johnson's payment token does not meet the criteria of the key string/authentication credential. In Johnson, the buyer only selects a payment provider using payment options (payment types). (EX1004 at [0016]), [0030]), [0099], [0100]) and uses the secured resource (bank account, debit card or credit card number) to pay for the payment token which indicates to the merchant that the payment provider holds the covering funds to pay the merchant for the transaction. In Johnson, the authorized user of the secured resource is not requesting the merchant to access it as it is in the '079 which contemplates the secured resource be used to complete a normal credit card transaction in which there is a single direct (but unguaranteed) transaction. Oglesby Decl. at ¶ 78.

Unlike the payment token provided to the buyer in Johnson (and the transaction code provided to the buyer in Stambaugh, the ‘079 does not need to provide the specific key string/authentication credential for the transaction to the authorized user, as this will already be known to the authorized user. Thus in the ‘079 the key string[5] is known to the user whereas in Johnson and Stambaugh it must be provided to the buyer.[6] Oglesby Decl. at ¶ 79.

D. Johnson Does Not Have "A Service User Interface In Communication With Said Server…To Receive Input From Said Unauthorized Service Client"

The ‘079 patent requires input from the unauthorized service client to the server which, along with the authentication credential, will be used to authenticate the transaction as having been requested by the authorized user. In a merchant transaction that input will be at least the merchant identifier and preferably the transaction amount. (See Ex1001 at 16:9 – 16:15) ("In any case, with the authentication credential provided, the fueling station, restaurant or on-line retailer submits in an authentication message the end user provided authentication credential to the service provider 36 along with the service client's identifying information 71 for validation and, assuming validation passes, access

[5] The storage, definition and usage of key strings is well documented throughout the ‘079. (EX1001 2:2-4; 3:25-28; 9:9-13; 13:58 – 15:65).

[6] The plain language of the claim does not include any requirement for the "key string" to be established prior to the initiation of the transaction and Petitioner points to no requirement from the specification or prosecution history that would require such a limitation.

to the end user's authorized secured resource-in this case payment.")

Thus the claim requires a service interface used to provide input from the unauthorized client in addition to receiving the authentication credential. The server evaluates the authentication credential to authenticate the identity of said requester through a comparison of the transaction data sent by the merchant with the transaction provided by the authorized user of the secured resource. Oglesby Decl. at ¶¶ 80-81.

As set forth above, Johnson's payment token is an authorized resource of the merchant on whose behalf the payment provider is holding the funds for payment. It is not a secured resource of the buyer. Thus, in Johnson's system, the payment token is received from the authorized service client (of the payment token), not an unauthorized service client. Johnson thus only requires the merchant provide the payment token in order for the payment provider to provide the funds held for the merchant. Johnson expressly teaches no authentication of the payment token is necessary. Moreover, the purpose of the optional validation step is to validate the token as a good indicator to the merchant of the payment guarantee. There is no disclosure in Johnson of the payment token being evaluated in any way to identify the buyer. Johnson instead has considerable description of evaluating an identity token to identify the buyer. Oglesby Decl. at ¶¶ 82.

In sum, Johnson discloses a system:

- In which a payment provider's server receives a user request to fund a payment guarantee issued by a payment provider for a specific merchant. It does not disclose a service provider's server authenticating a request from a buyer for the merchant to access a secured resource of the buyer, as required by the claim.
- In which a payment provider's server receives a payment token from a merchant. The payment token is used to release a payment held by the payment provider. The payment token is used to provide access to a secured resource of the buyer. Moreover, the payment token is not the claimed authentication credential because it does not meet the requirements for a key string/authentication credential and is not evaluated by the server to authenticate that an access request came from the buyer.
- In which transaction information is only provided from the merchant to the buyer. There is no disclosed interface between the server and the merchant to receive the input from the merchant besides the payment token, as required by claim 1 of the '079 patent. The '079 patent requires transaction information to be input to the server from both merchant and the buyer in order to validate the identity of

authorized user as the originator of the request.

1. The Combination of Johnson & Stambaugh Does Not Render Claim 1 Obvious.

A person of ordinary skill in the art would not be motivated to add Stambaugh's message authority to Johnson because it would not meet the trust boundary requirement of Johnson and actually be less efficient and effective since it would require too much manual information to be input by hand into a payment token request, but in any event, adding the message authority to Johnson would not help meet the requirement of claim 1 because of all the other ways Johnson fails to expressly or inherently meet claim 1. Oglesby Decl. at ¶ 84.

Therefore, adding Stambaugh's message authority to Johnson, even had a POSITA motivation to do so as Petitioner suggests, still would not meet this limitation. Moreover, a POSITA would not be motivated to add Stambaugh's message authority which is manual, prone to attack and involves more work on the part of the consumer, particularly given Jonson's payment token request is not necessarily compact as taught in the '079 patent, and may involve transmitting sensitive information. Oglesby Decl. at ¶ 85.

2. The Combination of Johnson & Stambaugh Does Not Render Claim 6 Obvious.

Claim 6 is dependent of claim 1 and adds the further requirement that the "second set of instructions includes instructions operable to invalidate said authentication credential based upon passage of time."

Johnson in view of Stambaugh does not raise a prima facie case that claim 6 is obvious for the same reason the asserted combination does not raise a prima facie case for claim 1, as I explained above. In particular, neither Johnson nor Stambaugh disclose the four party single payment transaction system claimed system of claim 1 or the claimed authentication credential used in the same way as claimed as those systems do not disclose or require access to an authorized user's secured resource to complete the transaction. Therefore, Johnson also does not render claim 6 obvious in view of Stambaugh Oglesby Decl. at ¶¶ 86-87.

3. The Combination of Johnson & Stambaugh Does Not Render Claim 7 Obvious.

Claim 7 is dependent of claim 1 and adds the further requirement that the "a second set of instructions operable to conduct for the benefit of said unauthorized service client a transaction reliant upon access to said secured resource."

Johnson in view of Stambaugh does not raise a prima facie case that claim 7 is obvious for the same reason the asserted combination does not raise a prima facie case for claim 1, as I explained above. In particular, neither Johnson nor Stambaugh disclose the four-party single payment transaction system claimed system of claim 1 or the claimed authentication credential used in the same was as claimed as those systems do not disclose or require access to an authorized user's secured resource to complete the transaction. Therefore, Johnson also does not render claim 7 obvious in view of Stambaugh. Oglesby Decl. at ¶¶ 88-89.

4. The Combination of Johnson & Stambaugh Does Not Render Claim 9 Obvious.

Claim 9 is dependent of claim 7 and adds the further requirement that the "transaction comprises providing a financial benefit."

Johnson in view of Stambaugh does not raise a prima facie case that claim 7 is obvious for the same reason the asserted combination does not raise a prima facie case for claim 1, as I explained above. Neither Johnson nor Stambaugh disclose the four party single payment transaction system claimed system of claim 1 or the claimed authentication credential used in the same was as claimed as those systems do not disclose or require access to an authorized user's secured resource to complete the transaction. Therefore, Johnson also does not render claim 9 obvious in view of Stambaugh. Oglesby Decl. at ¶¶ 90-91.

5. The Combination of Johnson & Stambaugh Does Not Render Claims 11, 16, 17, and 19 Obvious.

Each of these claims comprises the method analog of the system claims 1, 6, 7 and 9. Johnson in view of Stambaugh therefore does not raise a prima facie case that these claims are obvious for the same reasons I previously explained the asserted combination does not raise a prima facie case for the analogous system claims. Claim 1, as I explained above.   Neither Johnson nor Stambaugh disclose the four party single payment transaction system claimed method of claim 11 or the claimed authentication credential used in the same way as claimed, because those systems do not disclose or require providing access to an authorized user's secured resource to complete the transaction. Therefore, Johnson also does not render claims 11, 16, 17 and 19 obvious in view of Stambaugh. Oglesby Decl. at ¶ 92.

6. Summary of Conclusions Regarding Ground 1

Johnson in view of Stambaugh does not render claims 1, 6, 7, 9, 11, 16, 17, and 19 as obvious because, Johnson, the baseline reference, does not disclose the system and method of claim 1 and 11.

Johnson instead discloses a system:

- In which a payment provider's server receives a user request to fund a payment guarantee issued by a payment provider for a specific merchant. It does not disclose a service provider's server authenticating a request from a buyer for the merchant to access a secured resource of the buyer, as required by the claim.
- In which a payment provider's server receives a payment token from a merchant. The payment token is used to release a payment from the payment provider; not to provide access to a secured resource of the buyer. Moreover, the payment token is not the claimed

authentication credential because it does not meet the requirements for a key string/authentication credential and is not evaluated by the server to authenticate that the request came from the buyer.

- In which transaction information is only provided from the merchant to the buyer. There is no disclosed interface between the server and the merchant to receive the input from the merchant besides the payment token, as required by claim 1 of the '079 patent. The '079 patent requires transaction information to be input to the server from both merchant and the buyer to validate the identity of authorized user as the originator of the request.
- A person of ordinary skill in the art would not be motivated to add Stambaugh's message authority to Johnson because it would not meet the trust boundary requirement of Johnson and be less efficient and effective since it would require too much manual information to be input by hand into a payment token request, but in any event, adding the message authority to Johnson would not help meet the requirement of claim 1 because of all the other ways Johnson fails to meet claim 1.

Nor would a POSITA replace the efficient automated communicating process used in Johnson with the cumbersome error prone manual process of

Stambaugh and expose sensitive information like payment provider user id and password to exposure through to an SMS/text system. Oglesby Decl. at ¶¶ 93-95.

The asserted combination of Johnson in view of Stambaugh would not change the basic architecture and three-party double payment transaction protocol of Johnson to provide an on-line version of the bank demand draft model.

Johnson in view of Stambaugh would not change the basic requirement of Johnson which is limited to specific payment providers who must be financial institutions, whereas service provider in 079 can be any entity. Oglesby Decl. at ¶¶ 96-97.

Neither the payment token of Johnson nor the transaction code of Stambaugh meet the requirements for a key string in 079 patent. Nor would the asserted combination address that merchant presenting the payment token to the payment provider is already authorized to use the payment token without further authentication required, whereas the merchant providing the service provider in the ‘079 patent with an authentication credential in the ‘079 patent is an unauthorized service client wherein the authentication credential must be used to identify the authorized service client having approved the transaction before it can proceed. Oglesby Decl. at ¶ 98.

VI. THE COMBINATION OF JOHNSON, STAMBAUGH, AND

SELLARS CANNOT RENDER OBVIOUS CLAIMS 1, 3, 6-9, 11, 13, AND 16-19 OF '079 PATENT (GROUND 2)

1. The Combination of Johnson, Stambaugh and Sellars Does Not Render Claim 3, 13 Obvious.

Claim 3 is dependent of claim 1 and claim 13 is dependent of claim 11. Both respectively add the further requirement to "[determine] from among a plurality of secured resources associated with said authorized user the identity of a single secured resource to which said requester requests access."

Johnson in view of Stambaugh in further view of Sellars does not render claim 3 or 13 is obvious. Is previously discussed, Johnson in view of Stambaugh does not render claim 1 or 11 obvious because Johnson does not disclose the requirements of claims 1 or 11 alone or in view of Stambaugh.

In particular, neither of these references alone or in combination disclose a single payment-transaction protocol between a merchant and a buyer in which a value meeting the definition for the key string/authentication credential is known by the buyer and passed by the buyer to the merchant to be provided along with additional input from the merchant to the authenticator in order to authenticate the identity of the buyer as party who authorized the transaction. More particularly, none of these disclose an authentication credential which is associated with a secured resource and a merchant, does not include a common identifier for the resource or provide any knowledge that would provide ordinary access to the secured resource, cannot be used again without new authority from the buyer, and is determined based upon a request by an authorized user of a secured resource to provide to an unauthorized use of the secured resource access to the secured resource. Oglesby Decl. at ¶¶ 99-101.

The defects in Johnson alone or in combination with Stambaugh are not cured by adding Sellars. Petitioner asserts that Sellars would "enable the payment provider to determine which account, from among multiple accounts, the user is requesting for a given transaction…" Mott Decl. (EX1007), at ¶ 90.

However, the above justification is incorrect. In Johnson, the merchant accepts payment from selected payment providers, who are further restricted based upon the funding method by which the buyer is purchasing the payment token issued by the payment provider that is to be provided to the merchant to secure the release of the goods/services. Nothing in Johnson describes even the desire to support the user being able to choose between multiple card accounts with a single payment provider to pay for payment token for a given transaction. Oglesby Decl. at ¶¶ 102-104.

Assuming however that a POSITA would be motivated to modify Johnson's system to enable the user to be able choose from multiple card accounts to fund a given payment provider, adopting Sellars. In the '079 system, the key string/ authentication credential must be evaluated by the server to authenticate the identity of the authorized user as the one who approved the request. Only then is it used to look up the secured resource to complete the transaction. Indeed, the claim requires the ability for the merchant to also provide input besides the authentication credential so that the evaluation taught in the specification can take place.

Sellars in contrast teaches that each account can have a different encryption key and that which account is to be used is determined by which encryption scheme was used or by an account identifier concatenated within the credentials. (EX1006 [0234]). ("In some embodiments, if Carol holds multiple accounts for Bob each having account numbers x1, x2, ... , xn, Carol generates a hash for each account number. If one of the hashes can decrypt the credentials (Bcred), Carol knows which account to draw funds from. Bob can also prepend an account identifier to the credentials (Bcred) to identify a particular account.") No step of additional inputting or evaluating an authentication credential to identify the user is disclosed in Sellars. Oglesby Decl. at ¶¶ 105-106.

Sellars' topography is different in other ways from that claimed in the '079 patent. The buyer never provides an authentication credential to the vendor for the vendor to pass onto the authenticator. The vendor also does not provide an authenticator with an authentication credential to be evaluated to identify the buyer. Oglesby Decl. at ¶ 107.

Sellars depicts a commercial transaction in FIG. 21 and uses the names Bob, Vera, Carol and Trent to denote buyer, vendor, payment authenticator and authenticator respectively. The role for authenticator (Trent) is to provide transaction keys so that the three parties, buyer (Bob), vendor (Vera) and payment authenticator (Carol), can communicate securely without exposing sensitive information. Oglesby Decl. at ¶ 108.

The commercial transaction as shown in FIG.21 is explained in Sellars paragraphs [0283] to [0292]. Following is a brief description of such a commercial transaction:

- Buyer (Bob) and vendor (Vera) finalize a transaction
- Buyer (Bob) requests authenticator (Trent) for a transaction key to encrypt buyer’s account information.
- Buyer (Bob) sends encrypted buyer account information to payment authenticator (Carol)
- Vendor (Vera) requests authenticator (Trent) for a transaction key to encrypt vendor’s account information.
- Vendor (Vera) send encrypted vendor account information to payment authenticator (Carol)
- Vendor (Vera) digitally signs the finalized transaction and sends it to buyer (Bob).
- Buyer (Bob) digitally signs the finalized transaction signed by the vendor (Vera) and sends it to authenticator (Tent)
- Authenticator (Trent) sends a payment request based on the finalized transaction to payment authenticator (Carol).
- Payment authenticator (Carol) decrypts the payment request using mutating identifiers, withdraw finds from buyer’s (Bob’s) account, deposit

funds into vendor's (Vera's) account and send receipts to buyer (Bob) and vendor (Vera).

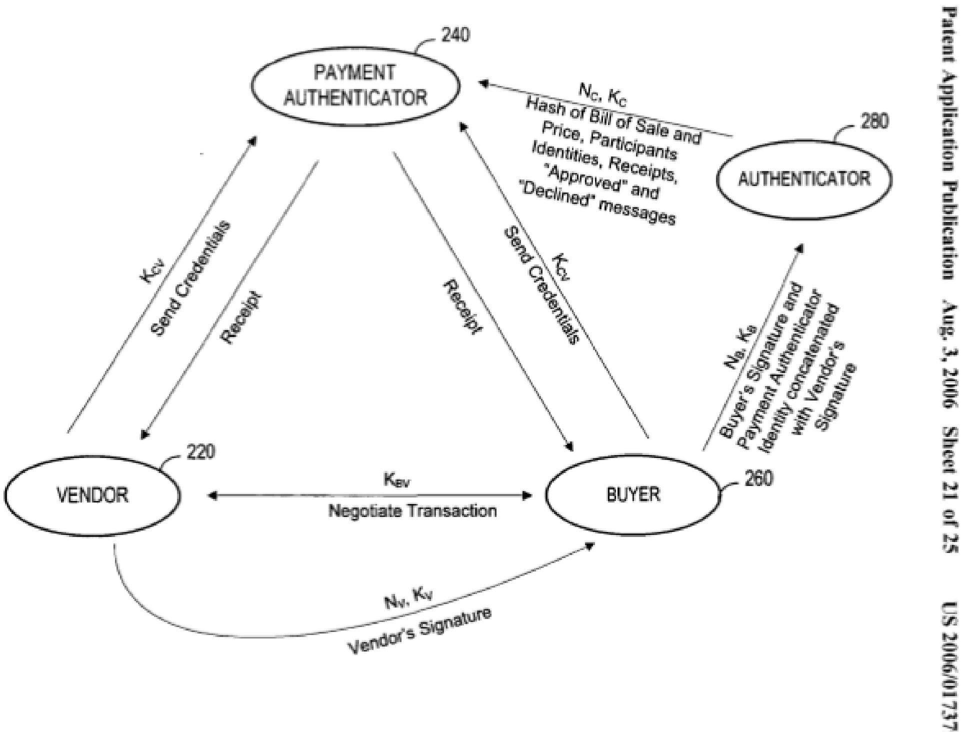
Patent Application Publication Aug. 3, 2006 Sheet 21 of 25 US 2006/0173794 A1
240
PAYMENT AUTHENTICATOR
280
AUTHENTICATOR
N_C, K_C
Hash of Bill of Sale and Price, Participants Identities, Receipts, "Approved" and "Declined" messages
K_{CV}
Send Credentials
Receipt
Receipt
Send Credentials
K_{CV}
N_B, K_B
Buyer's Signature and Payment Authenticator Identity concatenated with Vendor's Signature
220
VENDOR
K_{BV}
Negotiate Transaction
BUYER
260
N_V, K_V
Vendor's Signature

FIG. 21

Johnson combined with Stambaugh, as previously discussed, would result in text and SMS messages being sent from a mobile device to a payment provider of Johnson via the message authority of Stambaugh. Even, the purchaser would have to manually enter the payment token request into the text or SMS message.

Adding an account identifier to payment token request, as taught by Sellars, would make manual entry even longer and would compromise sensitive information that a POSITA would not be motived to transmit through a text or SMS message. Therefore, combining these three references is impractical. None of references (alone or in combination) would lead a POSITA to the claimed '079 system without making significant architectural modifications taught only in the '079 patent for at least all the reasons herein stated.

Johnson in view of Stambaugh in further view of Sellars thus does not render claim 3 obvious. Oglesby Decl. at ¶ 109-113.

2. The Combination of Johnson, Stambaugh and Sellars Does Not Render Claim 8, 18 Obvious.

Claim 8 is dependent of claim 7 and likewise claim 18 is dependent of claim 17. Each of these respectively adds the requirement to [generate] a receipt for said transaction and to [transmit] said receipt to said authorized user."

Johnson also does not disclose the requirements of claim 7 or 17 alone or in view of Stambaugh. In particular, none of these alone or in combination disclose a single payment-transaction protocol between a merchant and a buyer in which a value meeting the definition for the key string/authentication credential is known by the buyer and passed by the buyer to the merchant to be provided along with additional input from the merchant to the authenticator in order to authenticate the identity of the buyer as party who authorized the transaction. More particularly, none of these disclose an authentication credential which is associated with a secured resource and a merchant, does not include a common identifier for the resource or provide any knowledge that would provide ordinary access to the secured resource, cannot be used again without new authority from the buyer, and is determined based upon a request by an authorized user of a secured resource to provide to an unauthorized use of the secured resource access to the secured resource.

Adding Sellars to the combination does not render claims 8, 18 obvious for the same reasons set for above in connection with claims 3, 13. Oglesby Decl. at ¶ 114-116.

VII. CONCLUSION

None of the references raised in the Petition, whether alone or in any alleged combination, teach the claimed system and method of the '079 patent. In particular, none of these alone or in combination discloses a system or method in which an authorized user (*e.g.* consumer) requests access for an unauthorized service client (*e.g.* a specific merchant) to a specified secured resource (*e.g.* a given credit card number designated by the consumer to be used to process the transaction) in which a key string associated with the transaction known to the authorized user and service provider (*i.e.* authenticator) is used to make an authentication credential passed by the authorized user to the unauthorized service client to be provided, along with additional input from the unauthorized service client in order to authenticate the identity of the authorized user as the party who authorized the transaction, wherein authentication credential associated with the transaction does not include a common identifier for the secured resource, provide any knowledge that could be used to gain ordinary access to the secured resource, and cannot be used again without new authority from the authorized user of the secured resource. As such, none of the references can render any claim of the ‘079 Patent obvious, and Petitioner cannot establish a reasonable likelihood that at least one of the challenged claims is unpatentable. Accordingly, *Inter Partes* review should not be instituted, and the Petition should be denied under 35 U.S.C. §314(a).

Respectfully submitted,

/ Sandeep Seth /
Sandeep Seth, Reg. No. 37,537
SETH LAW OFFICES

Date: March 9, 2017

CERTIFICATION OF WORD COUNT

The undersigned hereby certifies that the portions of the above-captioned PATENT OWNER'S PRELIMINARY RESPONSE specified in 37 C.F.R. §42.24 has 13,541 words, in compliance with the 14,000 word limit set forth in 37 C.F.R. § 42.24. This word count was prepared using Microsoft Word 2013.

/ Sandeep Seth /
Sandeep Seth, Reg. No. 37,537
SETH LAW OFFICES

Date: March 9, 2017

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the following documents were served on March 9, 2017 by electronic service in accordance with the consent to electronic service on pages 72-73 of the Petition for Review in this proceeding:

PATENT OWNER’S PRELIMINARY RESPONSE UNDER 37 C.F.R. § 42.107

The names and email addresses of the parties being served are as follows:

Unified Patents, Inc.
jason.mudd@eriseip.com
eric.buresh@eriseip.com
ptab@eriseip.com
jonathan@unifiedpatents.com

/ Sandeep Seth /
Sandeep Seth, Reg. No. 37,537
SETH LAW OFFICES

Date: March 9, 2017